Refocusing risk governance

Last year's overhaul of the UK Corporate Governance Code has important and far-reaching implications for both boards and risk managers

BY MARK BUTTERWORTH

More than 25 years ago we saw the publication of the first UK Corporate Governance Code (the Cadbury Code), and it's fair to say that since then corporate governance practices have never stayed static for long – with updates largely every two years over that period. But in the Code update consultation process for 2018 announced by the Financial Reporting Council, notice was given that this time meaningful changes were planned. Not all of the changes floated in the consultation were carried through to the published edition, but notable areas of governance development were readily supported and adopted.

Risk managers will need to consider how they will adjust their risk management practices to ensure the emerging or upgraded features of the new Code receive appropriate focus. While culture management has been high on the governance and risk agenda for a number of years, the formalisation of Code expectations means there is more that risk managers should be doing in terms of tangible risk culture actions.

> The challenge to the risk function is to build a relationship with workforce representatives that results in effective two-way communication

Risk culture

The main thrust of risk culture management is designing and applying culture metrics upon which the risk function

Reprinted courtesy of Enterprise Risk magazine and the Institute of Risk Management

The formalisation of Code expectations means there is more that risk managers should be doing in terms of tangible risk culture actions

can create purposeful reports to senior managers and the board. These metrics may include accident and other risk events, staff turnover and absenteeism relative to industry norms, attendance at required training sessions and customer complaints and actions taken following audit recommendations. Risk culture profiling tools are now available and should be adopted by risk managers who wish to build a base case of culture and apply periodic improvement assessments. Such tools also provide a quantified platform for discussion with the board, rather than soft factors alone.

Risk managers have a clear understanding that in order to sustain an enterprise-wide approach to risk management they need to consider the risk perspectives of all stakeholders – these might be shareholders, regulators, suppliers and customers, and many more. The 2018 Code now requires boards to engage with the workforce and to use one or a combination of three methods: a director appointed from the workforce, a formal workforce advisory panel and/or a designated non-executive director.

The advantages this could bring to risk management are formalised routes for the workforce to raise concerns about operational risks and the design and effectiveness of the control environment. Also, any concerns about the culture within the organisation can be aired through workforce liaison. However, the challenge to the risk function is to build a relationship with workforce representatives that results in effective two-way communication. The risk manager may have to introduce a broader risk management induction programme and develop the internal risk-briefing approach so that the risk strategy is clearly understood by all concerned, and conversely the workforce views on risk appetite are shared with the risk manager.

Effectiveness

A significant feature of the 2018 review and consultation has been the elevation of the FRC's Guidance on board effectiveness to a position that should be regarded as of equal importance as the Code itself. The stated aim of the FRC to "shorten and sharpen" the Code resulted in some important governance requirements being transferred to the updated guidance. Risk managers will need to have a detailed awareness of the guidance and develop risk management strategies that link clearly with board operations. In fact, the guidance goes beyond simply providing a checklist of must-do's by boards and leads directors to ask what circumstances, or risks, can result in below-standard board effectiveness.

Greater importance has been given to evaluation of board performance (or "effectiveness"), with a formal and rigorous internal annual review (often a short questionnaire-based review by the company secretary), as well as the all-important independent external evaluation. Ideally this should take place every two or three years and be carried out by a governance specialist with no conflicts of interest – certainly not your external auditor.

This external review should allow the reviewer to have direct contact with all directors, plus certain key individuals such as the head of audit, company secretary and head of risk management. But why are these reviews of such importance to the risk manager? The answer lies in the analysis of corporate

Reprinted courtesy of Enterprise Risk magazine and the Institute of Risk Management

The risk manager must place board reviews high on the list of key actions to be carried out each year, with a clear time frame and an appropriate budget

failures (or significant stress), where commentators often cite an ineffective board as the core reason for the problems. Better boards can be expected to address their operations in a structured and diligent way, with the risk culture clearly stated and complied with by all concerned.

Ownership

The question arises as to who owns the board evaluation process and makes sure it is carried out at the right time and with an appropriate agenda and thoroughness. While company secretaries have a traditional role here, it is the risk manager that has the greater interest in the evaluation findings and actions that are recommended. Therefore, the risk manager must place board reviews high on the list of key actions to be carried out each year, with a clear time frame and an appropriate budget. The role of the chair is made paramount in acting on the results of the evaluations and being prepared to report to stakeholders details of the process undertaken and the external firm used.

Those firms who undertake regular external board performance evaluations may well find to their advantage that they are able to demonstrate to their directors' and officers' liability insurers that the governance culture warrants the best terms possible. Risk managers whose role includes managing the business insurance programme will be keen to demonstrate value through lower premiums and good standards of cover.

Guidance on board effectiveness also emphasises that the board is responsible for setting the company's purpose and that "a well-defined purpose will help companies … articulate their approach to risk". The risk function needs to have regular and productive lines of communication with the board and provide high-quality risk analysis and reporting.

Another challenging implication of the 2018 Code is the more demanding role for the remuneration committee of the board and the remuneration framework. The FRC's emphasis is on ensuring the remuneration policies and practices are closely aligned with the long-term success of the organisation and play their part in delivering the firm's strategy. Risk managers must assess the degree to which remuneration structures incentivise the right behaviours, particularly in sales and client service. Also, given the increased responsibilities of the remuneration committee, more frequent interaction between the risk function and the chair and members of the committee (such as risk brainstorming) should be introduced.

Succession planning

The risk manager should keep a close eye on board succession planning and diversity in the board appointment pipeline. Commentary on the new Code has noted the need for diversity to start with upcoming managers and potential future directors. The importance of developing a diverse range of skills, experiences and outlooks for an effective board is well established – what the risk manager will focus on is the coherence of the attitudes to risk and the ability to build a unified risk strategy that is bought into by all members of the board. Risk managers may well add a new risk to their risk inventory – the failure to develop a diverse management team – with the consequences ranging from negative publicity and an unhappy workforce to losing market position as other organisations capitalise on the benefits diversity brings.

The UK corporate governance code has been widely emulated across the world (perhaps less so in the US), and it is sensible to expect the same for this edition. Non-UK regulators are likely to set higher standards for board effectiveness – linking strategy and risk more closely and setting more detailed risk reporting requirements.

The 2018 revisions to The UK corporate governance code have introduced relatively few changes to the specific section on audit, risk and internal control. Risk managers should, however, see the wider changes as an expansion of the concept of a risk management maturity model, where new risk and governance approaches, relationships, risk analysis and monitoring and reporting are all enhanced. In particular, firms must report how they are addressing emerging risks, as well as discuss the principal risks and uncertainties. Tracking the organisation's progress on a risk maturity model enables the risk function, as well as the board, to set a plan of action that will deliver a more resilient and productive firm, with a clear risk strategy. The risk picture is expanding and with it the expectation for broader business skills from risk managers and the ability to work at a strategic level, with all members of the board.

Mark Butterworth is managing director of the governance and risk consultancy Condie.

Reprinted courtesy of Enterprise Risk magazine and the Institute of Risk Management